

FIG. 1 Detective .. "Bogus" Load Modules Can Cause Problems

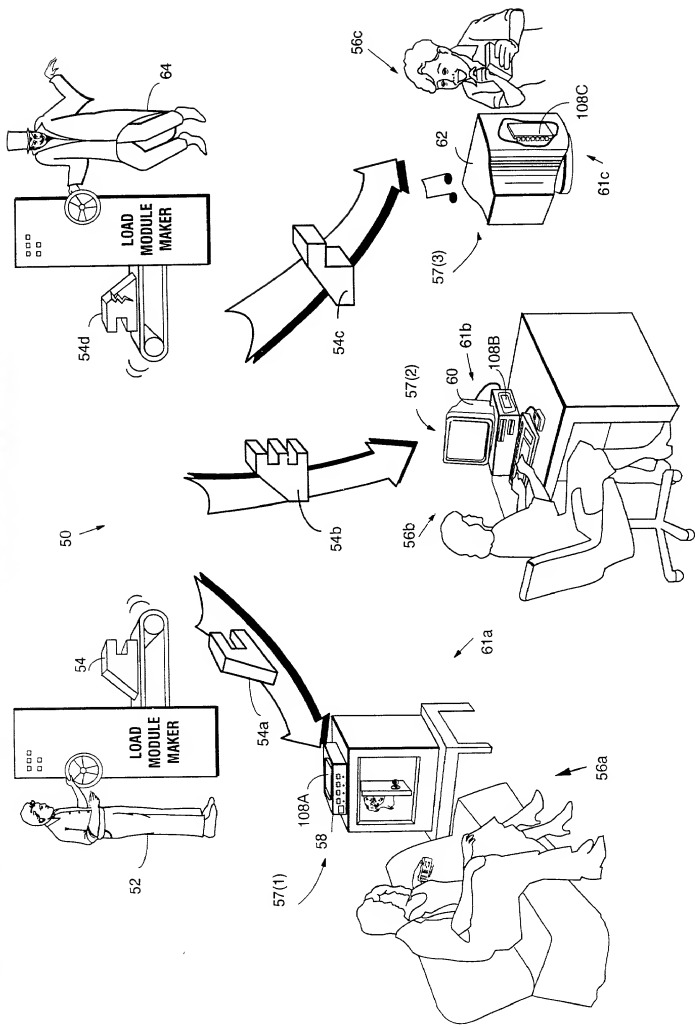


FIG. 2 Verifying Load Modules

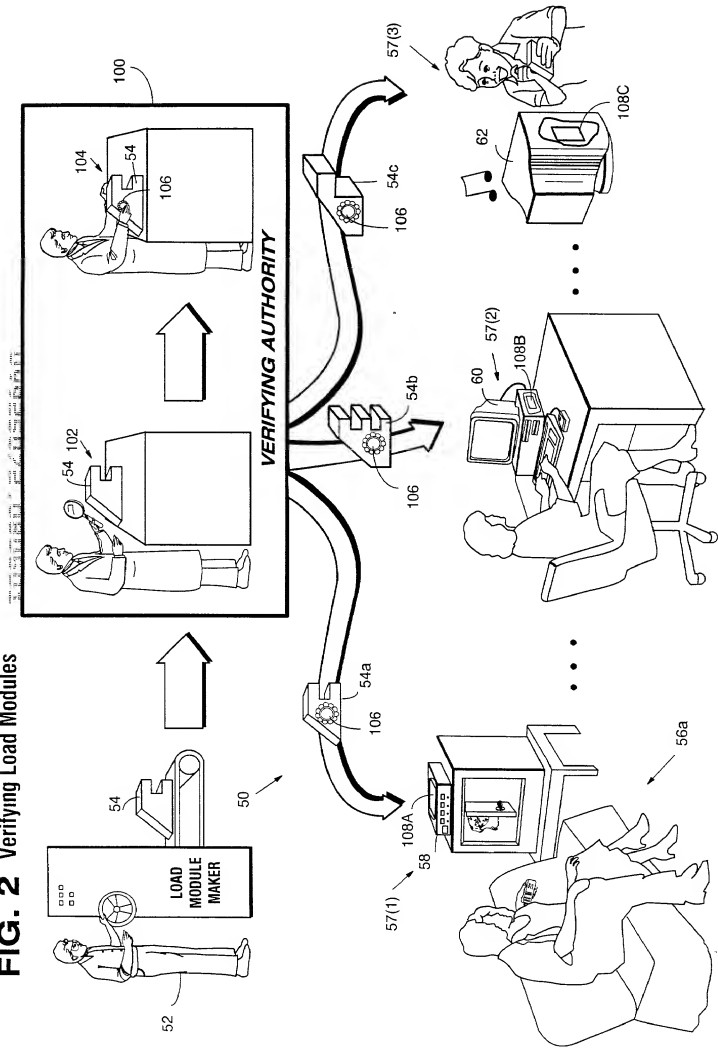
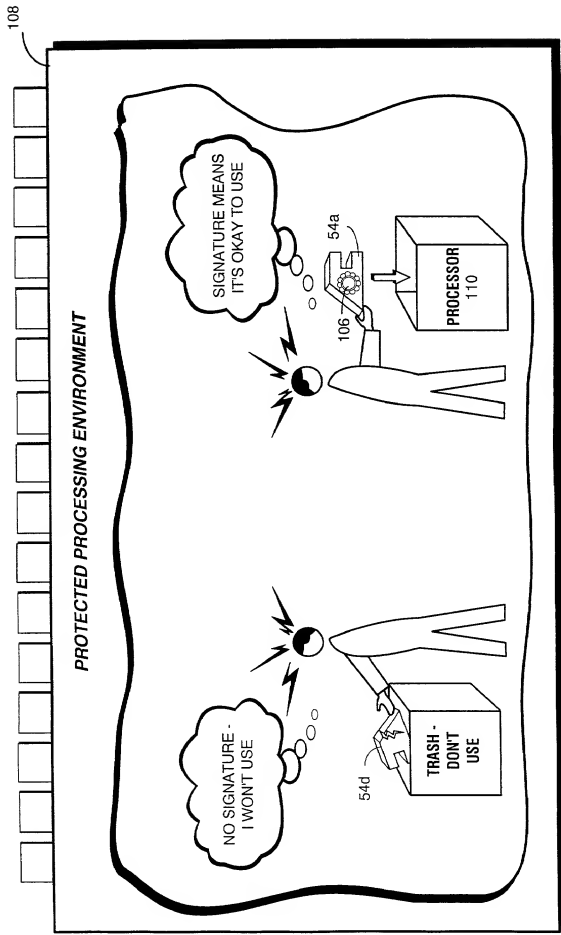


FIG. 3 Before Protected Processing Environment Uses A Load Module, It Checks To See If Load Module Has Been Verified



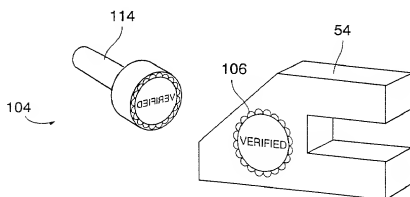
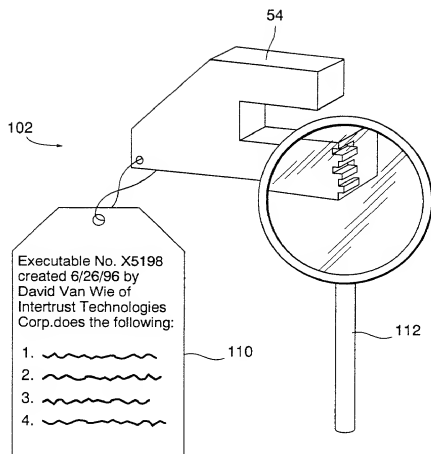


FIG. 4

**Certifying Load Module by
 Checking it Against its Documentation**

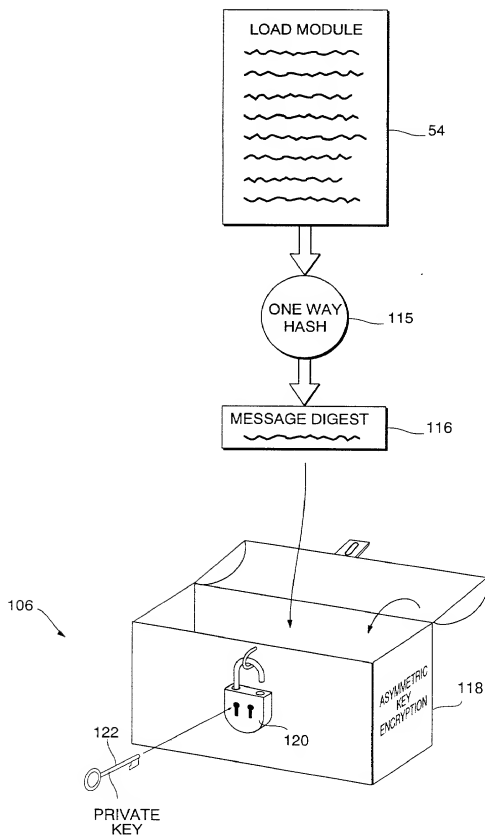


FIG. 5
Creating a Certifying
Digital Signature

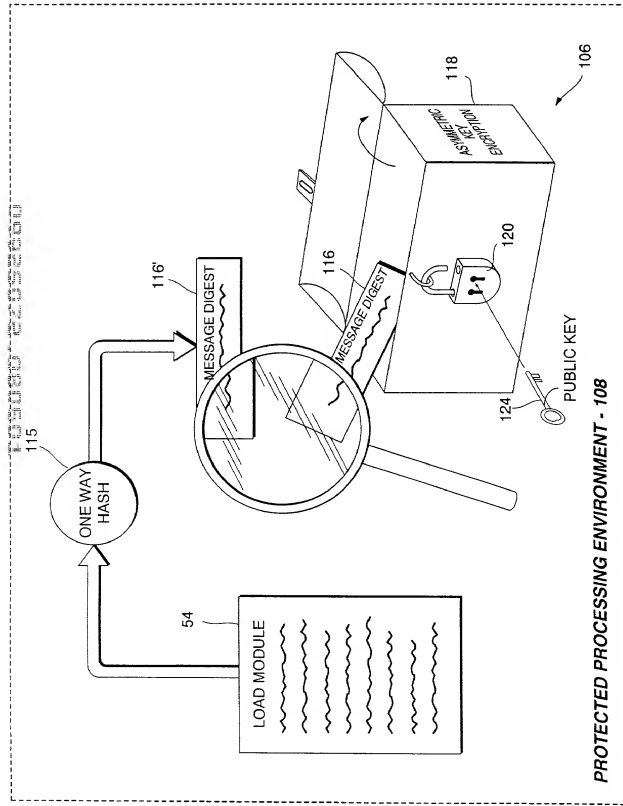


FIG. 6 Authenticating a Digital Signature

FIG. 7 Same Load Module Can Be Signed With Different Techniques

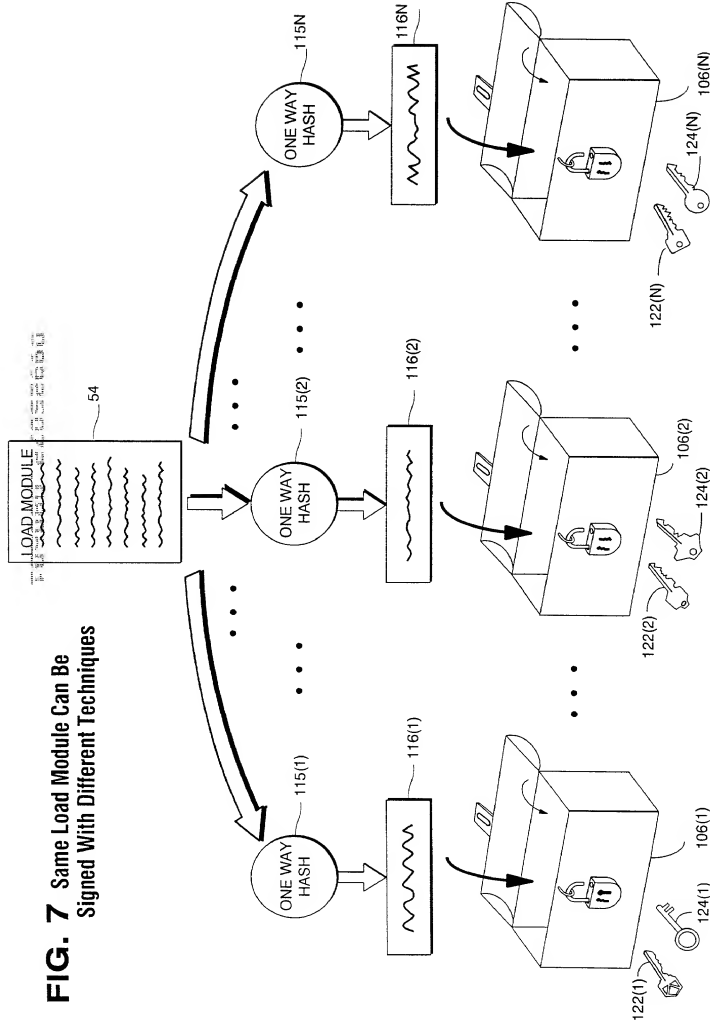


FIG. 8 Same Load Module Can Be Distributed with Multiple Signatures

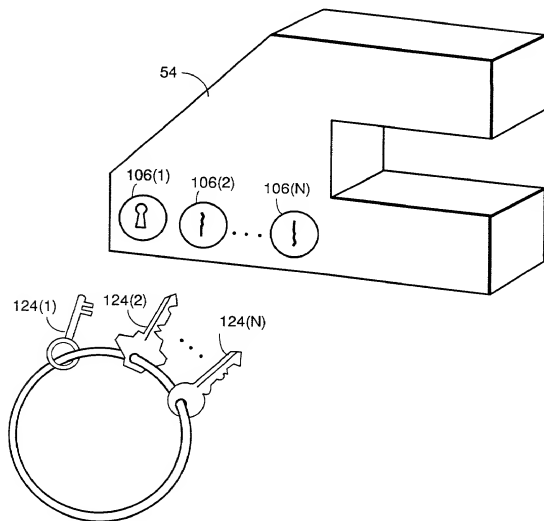


FIG. 8A Different Processing Environments Can Have Different Subsets of Keys

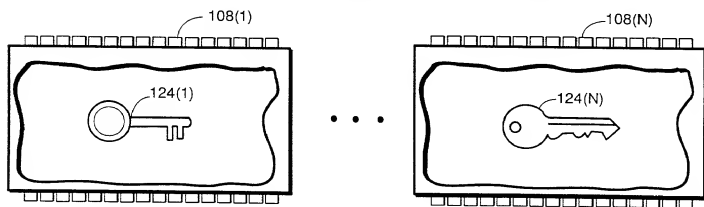
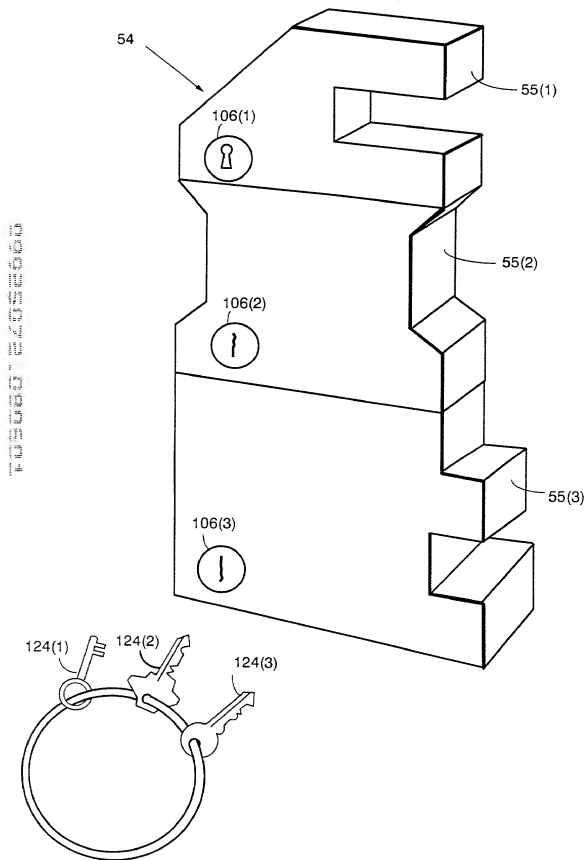


FIG. 9 Load Module Can Have Several Independently Signed Portions



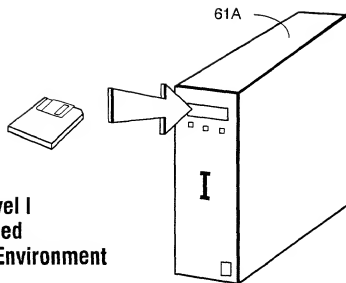


FIG. 10A Assurance Level I
Software-Based
Protected Processing Environment

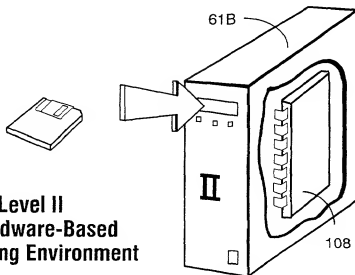


FIG. 10B Assurance Level II
Software and Hardware-Based
Protected Processing Environment

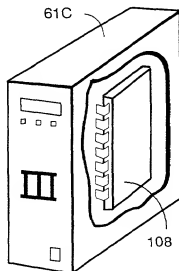


FIG. 10C Assurance Level III
Hardware-Based
Protected Processing Environment

FIG. 11A Level I
Digital Signature

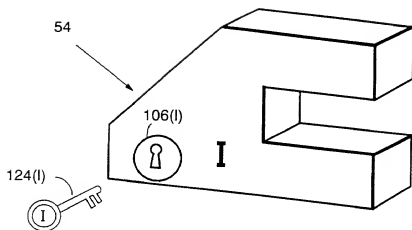


FIG. 11B Level II
Digital Signature

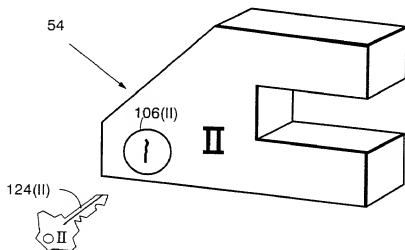
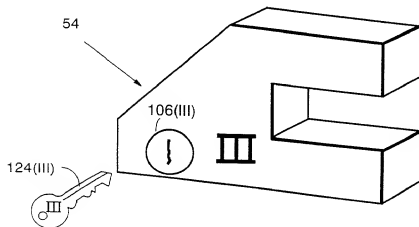


FIG. 11C Level III
Digital Signature



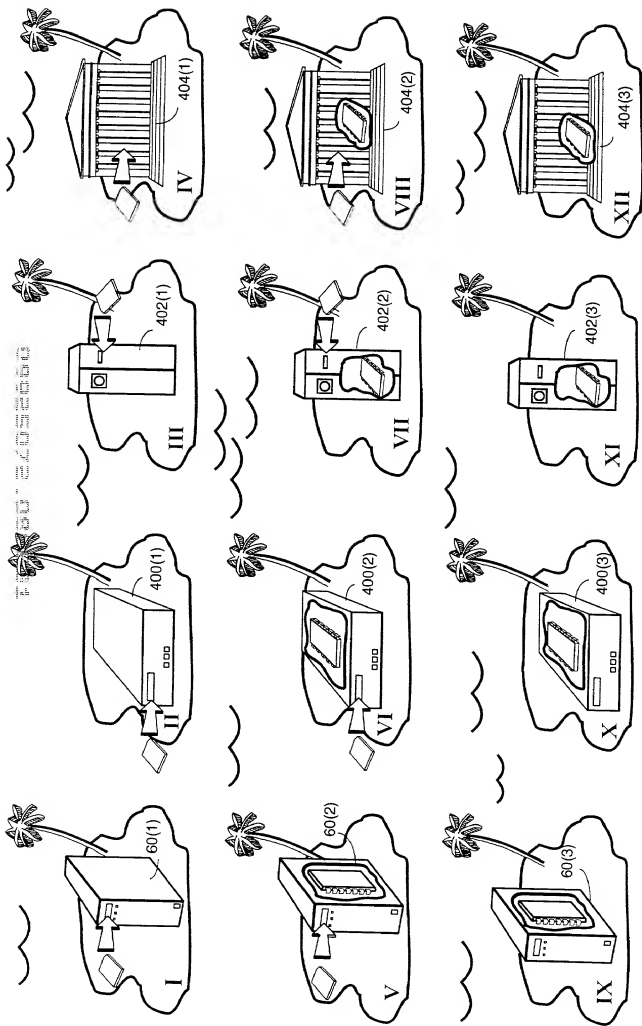


FIG. 12 Using Digital Signatures For Compartmentalizing Different Assurance Levels

FIG. 13 Multiple Assurance Levels

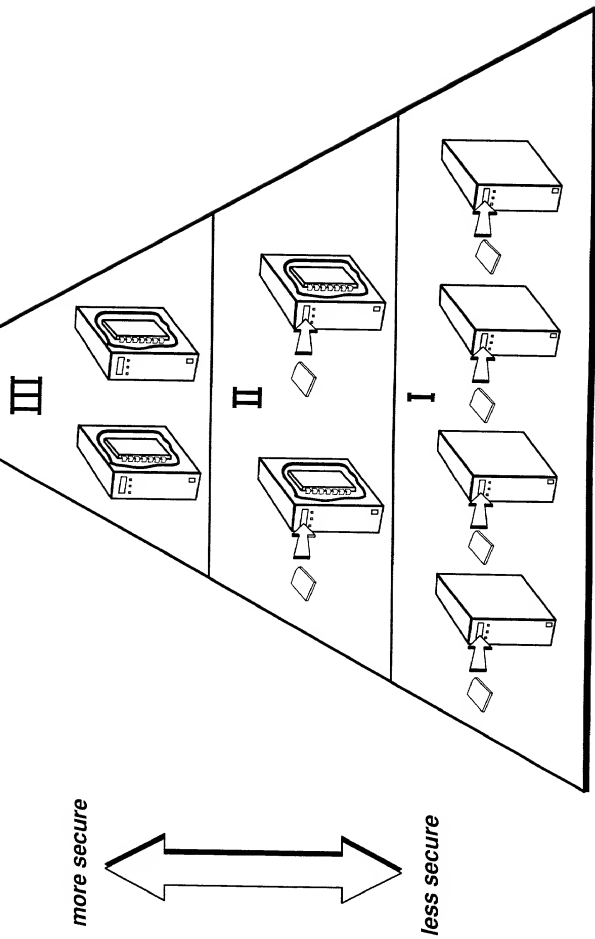
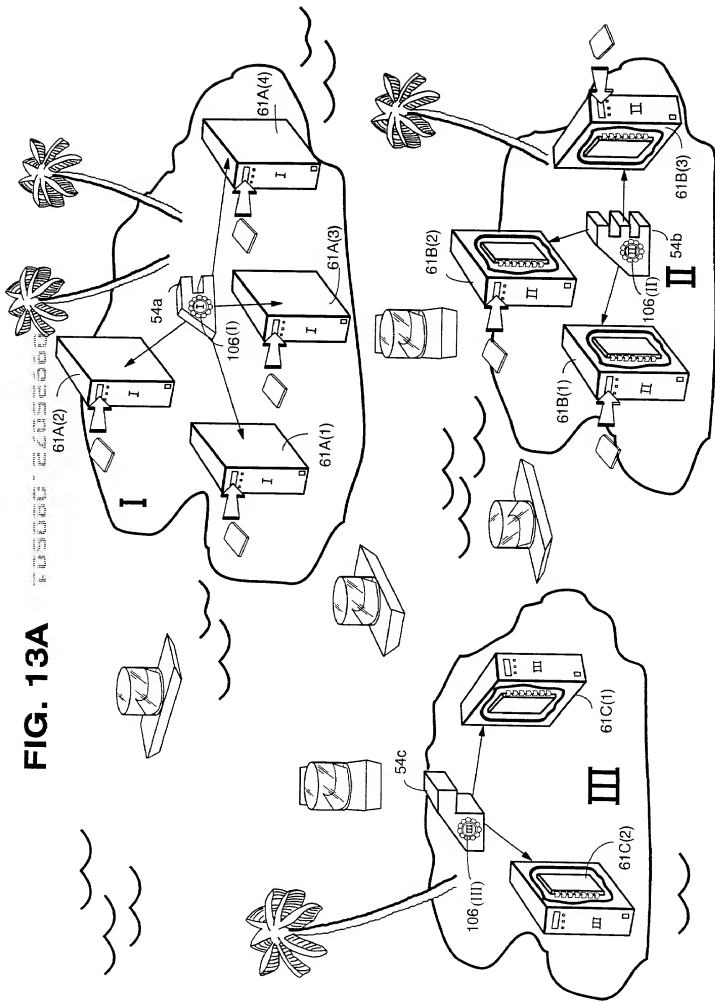


FIG. 13A



*Provider of
Executables*

FIG. 14

